Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.

© Clearwater Compliance | All Rights Reserved

CLEARWATER

Monthly Cyber Briefing

February 2023

Moderator: Jenny Davis

© Clearwater Compliance | All Rights Reserved

Mac McMillan
Founder & Advisor
CynergisTek, a Clearwater Company

Dave Bailey
VP, Consulting Services
Clearwater

Steve Akers
CTO, Managed Security Services
CISO
Clearwater

© Clearwater Compliance | All Rights Reserved

CLEARWATER
Not intended for public release

CYNERGISTEK
A Clearwater Company

TECH LOCK®
A Division of Clearwater

Cyber Update

Mac McMillan

RECENT CYBER EVENTS

Healthcare continued to be **targeted by hackers** both directly and indirectly as evidenced in the reported attacks at Toronto Health System, Jefferson County health Department, university of Miami Health, West Oaks Eyecare, AFLAC Insurance, Mscripts, Fitzgibbon Hospital, Satellite Healthcare, Captify Health and University of Colorado Hospital Authority. Needless to say, vigilance is still the order of the day.

Norton Lifelock notified almost a million users that their personal data had been compromised in a hacking incident. The attack involved "credential stuffing" an attack that utilizes previously exposed credentials on other sites and is effective because many users reuse the same username and password multiple times. Attackers may have had access to Norton's **Password Manager** which would have given then access to many other accounts. We have met the enemy, and it is us.

CISCO warns of a critical vulnerability that affects small business VPN routers. ***These are discontinued routers.*** A successful exploit can allow the attacker to authenticate and gain root access to the router's underlying operating system. Cisco will not release any updates to address this issue. There are approximately 19,500 of these devices still connected to the internet, nearly 5000 of them in the US. Which foot should I shoot?

© Clearwater Compliance | All Rights Reserved

CLEARWATER

Not intended for public release

CYNERGISTEK. A Clearwater Company

TECH LOCK® A Division of Clearwater

THREAT UPDATES

THREAT INSIGHT

Researchers and threat hunters have reported up to a **50% increase** in cyber attacks. Break out time for most attackers remains **less than 2 hours** making detection and reaction times for victims critical. The FBI has successfully **infiltrated HIVE and taken down its leak site** and disrupted thousands of attacks. HIVE extorted over $100M from healthcare.

VULNERABILITIES

Crowdstrike, reviewing data from its Falcon Overwatch product, identified a continuing **trend away from malware related attacks.** They attributed this to attackers having **valid credentials** to exploit. This makes it harder for defenders to recognize placing more emphasis on detecting anomalous activity which requires active monitoring.

HUMANS

Users are increasingly targeted in multiple and new ways. **Phishing campaigns** are still a go to initial approach for many attackers with phishing messages becoming more sophisticated and harder to detect. **Scanning QR codes** can lead to compromise. **Reuse of credentials** (same ID/password) on multiple sites, etc.

CHALLENGES

New on the enforcement front. For the first time the **FTC will sanction GoodRX** with a $1.5M fine and an order barring them from sharing user's sensitive healthcare data with third-party advertisers under it's Health Breach Notification Rule. GoodRX shared users data with Facebook, Google and Criteo for advertising purposes.

© Clearwater Compliance | All Rights Reserved

CLEARWATER

Not intended for public release

CYNERGISTEK. A Clearwater Company

TECH LOCK A Division of Clearwater

CYBER RESILIENCE

Meshing Proactive with Reactive Security to Achieve Superior Readiness

- COMMON SENSE: Simply put, you need both to be effective in today’s threat environment.
- PROACTIVE: Rethinking how we approach how we architect our security ecosystem. Overcoming reliance on static break the glass controls.
- REACTIVE: Planning, equipping, training, partnering, testing, evaluating – building the muscle memory that permits rapid action, precision and agility in response .

© Clearwater Compliance | All Rights Reserved

Not intended for public release

COMBATTING CYBER THREATS SMARTER

PREPARING FOR THE WIN

Execute your plan, not your adversaries plan

- **“Victory without fighting is the most advantageous way to win”**, Sun Tzu, General, Military Philosopher
- “Know your enemy and know yourself”. Effective defenses are built on understanding what we are trying to protect and repel.
- Tactics without strategy is the noise before defeat. You need a plan and preferably before throwing resources at the problem.
- The best defense is a good offense. Being proactive from a foundation of a good defense, always makes you stronger.
- **Cyber attackers like other criminal elements are interested in opportunistic exploits, speed and anonymity.**

© Clearwater Compliance | All Rights Reserved

Breaking the Reactive Cybersecurity Cycle through Hybrid Resiliency

Steve Akers & Dave Bailey

Presenters

Dave Bailey, CISSP

VP, Consulting Services

- Served as the Director of Technology & Security at Mary Washington Healthcare
- 12+ years of healthcare cybersecurity experience & 12+ years of experience serving in the Air Force

Steve Akers

CTO, Managed Security Services
Corporate CISO

- 25+ years of experience in the cybersecurity and compliance space
- 15+ years Security & Consulting Services
- U.S. Army, Army Reserves, National Guard – Medic and Military Police

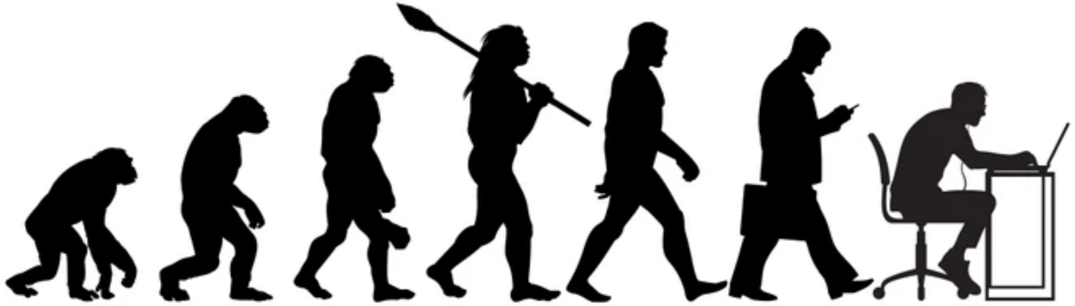
© Clearwater Compliance | All Rights Reserved

CLEARWATER CYNERGISTEK A Clearwater Company TECH LOCK A Division of Clearwater

Not intended for public release

Evolution: History

- Early days of Information and IT Security were grounded in physical security
  - Locks, Man Traps, Guarded Doors, Vaults – “Cyber” was not a thing
  - Networks were around years before firewalls
    - We are trying to share information, why would we want to block it
- Two paths on original firewalls – 1) Stop things coming in - DEC 2) Keep anything from getting out - AT&T
- ARPANET then the Internet -> Packet Filter vs Stateful Inspection
- Virus -> AntiVirus
- Stateful -> Application Layer – Application Firewalls
- AV -> NGAV
- NGAV -> EDR
- IT -> IT Security -> Information Security -> Cybersecurity



© Clearwater Compliance | All Rights Reserved

Proactive vs Reactive: *Reactive*

Reactive – In response to, following a cyberattack or breach

- Examples
  - Incident Response
  - Forcing password resets
  - Turning up paranoia dial
  - Forensics
- Manage threat and damage focus
- Response can help prevent similar future attacks
- Minimize damage and reduce costs
- *Without proactive, threat landscape is too large*
  - Too many corks in the bathtub
  - Not enough time for strategic thinking and planning

© Clearwater Compliance | All Rights Reserved

CLEARWATER

Not intended for public release

CYNERGISTEK
A Clearwater Company

TECH LOCK
A Division of Clearwater

Proactive vs Reactive: *Proactive*

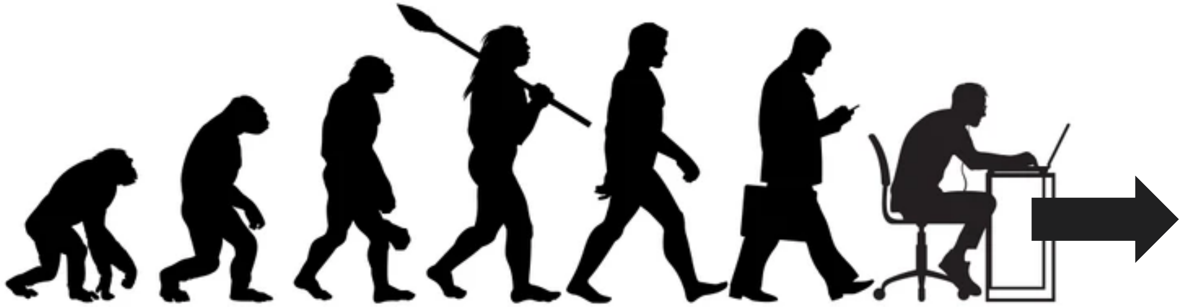
Proactive – Preempt, Predict, Identify Before

- Examples
  - Pen Testing and Threat Hunting
  - Awareness training
  - Unsupervised machine learning
  - Anomaly detection
- Prevention focus
  - Best defensive position
- Reduces impact and dwell times
- Largest technical investments in this space
- Reduce burnout of responders
- Improve compliance
- Detect inside job and mistakes
- *Without Reactive, can only go so far*
  - There is no 100% Secure

© Clearwater Compliance | All Rights Reserved

Evolution: Hybrid

- Modern threats require a modern approach to cybersecurity
  - *Proactive AND Reactive*
- Investments in time and resources for both is required
- Focus on the outcomes you want to achieve to drive strategy and growth for both
- Recognize the limitations of your organization
  - Technical capabilities
  - Staff skill set, time, other responsibilities
- Threats, attackers are changing – you must change too
- Just like the evolution of cybersecurity, it will take time
  - Reasonable and appropriate progress is the measuring stick for long-term resiliency



© Clearwater Compliance | All Rights Reserved

Not intended for public release

How do you evolve and grow to become more resilient? TAVE

TRACEABILITY

Ability to track from any event back to the point of origin and know who did what/when

ACCOUNTABILITY

Ability to impart trust and measure that people, processes, and technologies are executing the proper safeguards

VISIBILITY

Ability to see actively what is happening in the moment

ENFORCEABILITY

Ability to control or apply rules in order to achieve desired outcomes

© Clearwater Compliance | All Rights Reserved

Not intended for public release

How to apply TAVE

Response / Approach	Threat Vectors	People	Network	Endpoints	Software
Proactive	Traceability	- Awareness Training - Logging of Events	- Logging of Events	- Logging of Events	- Logging of Events
Reactive		- Alerting of Events	- Alerting of Events	- Alerting of Events	- Alerting of Events
Proactive	Accountability	- Testing Awareness - Phishing Exercises	- Segregation of Duties (SOD) Policy	- CIS Benchmarks	- Source Code Repositories
Reactive		- Flagging something as Spam/Phish	- N/A	- N/A	- N/A
Proactive	Visibility	- Password Manager	- Change Management	- Endpoint Detection and Response - Threat Hunting	- Code Review - Pen Testing
Reactive		- Alerting on Active Behaviors	- IDS	- Managed Detection and Response	- N/A
Proactive	Enforceability	- Multi-Factor Authentication	- Access Control Lists aligned with SOD - Firewalls	- Vulnerability and Configuration Management	- Change Management - SDLC
Reactive		- Mass Password Changes	- Auditing of SOD	- Patching	- Patching

*Meant as example only

© Clearwater Compliance | All Rights Reserved

Considerations for TAVE

No such thing as protect what’s important

Ask questions and challenge what’s being done across entire organization

Shoot for consistent and centralized security implementations so you can avoid:

- Different Protections
- Different Data
- Different Results

Work with a trusted third party to evaluate your risk exposure and security posture

- If everyone is doing everything right – what’s the risk?
- More than just a pen test

Understand, in detail, how would you and your organization respond to breach

Leverage trusted third parties to fill in gaps

© Clearwater Compliance | All Rights Reserved

Key Focus Areas

- Identify a baseline of network operations
- Implement detection processes into change management procedures; understand how change is going to impact detection and response
- Validate the effectiveness of implemented controls – i.e., red team, security control validation
- Partner collaboration throughout the lifecycle: configuration reviews, health checks
- Stay on top of the threats and understand how that influences and determines risk

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Why: NIST Cybersecurity Framework (CSF) Guidance

Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

- **Anomalies and Events**: Anomalous activity is detected, and the potential impact of events is understood
- **Security Continuous Monitoring**: The information System and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures
- **Detection Processes**: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

© Clearwater Compliance | All Rights Reserved

CLEARWATER

Not intended for public release

CYNERGISTEK
A Clearwater Company

TECH LOCK
A Division of Clearwater

In Summary

1. Neither Proactive nor Reactive can exist standalone in a modern risk management program
2. Proactive provides more scalability
3. Reactive provides best options to minimize damage if an event happens
4. Recognize gaps in your organization's limitations and seek the help of a trusted partner
5. A balanced, well thought out Hybrid approach across the many attack vectors will maximize resiliency

© Clearwater Compliance | All Rights Reserved

Mac McMillan

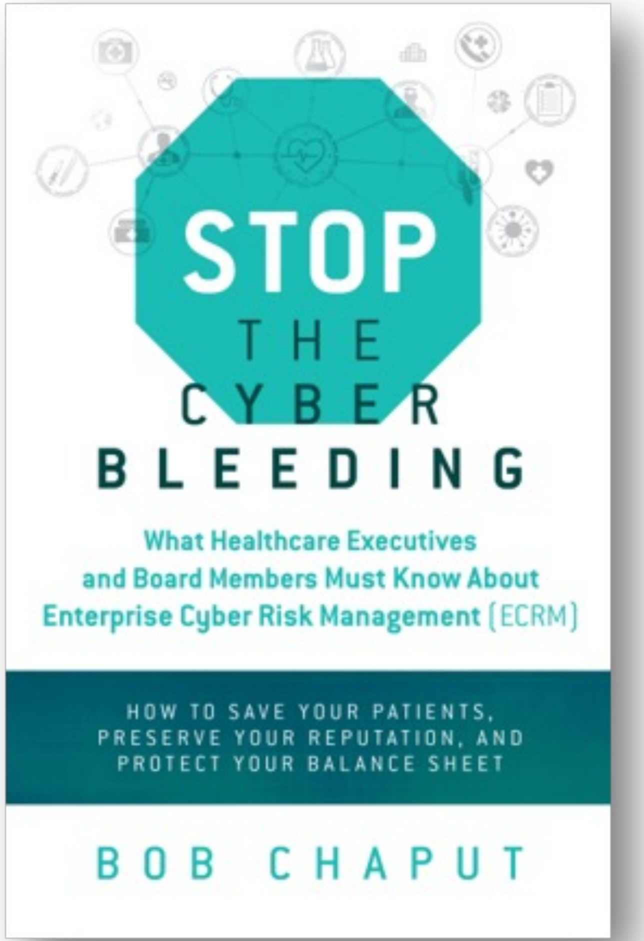
Dave Bailey

Steve Akers

© Clearwater Compliance | All Rights Reserved

Additional Educational Resources…

A Must-Watch Series for Healthcare Leaders


STOP THE CYBER BLEEDING
What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)
HOW TO SAVE YOUR PATIENTS, PRESERVE YOUR REPUTATION, AND PROTECT YOUR BALANCE SHEET
BOB CHAPUT

Available in digital, paperback, &, audio format.

https://amzn.to/33qr17n

CLEARWATER

HEALTHCARE CYBER RISK MANAGEMENT

CYNERGISTEK

A Clearwater Company

TECH LOCK®

A Division of Clearwater

© Clearwater Compliance | All Rights Reserved